A2 cont

116. (New) The method of claim 113 wherein the first session keys and the second session key are the same as each other.

REMARKS

Claims 1-53 have been canceled without prejudice. Claims 54-116 have been added. In view of the above amendments and remarks that follow, Applicant respectively requests favorable consideration and timely indication of allowance.

The Examiner has objected to the drawings. According to the Examiner, elements 1-10 in FIG. 2, and elements 50 and 1180 in FIG. 12 are not labeled. In response, attached hereto as Exhibit A are reproductions of FIGS. 2 and 12, as originally filed, with the elements specified by the Examiner circled in red. These drawings are being submitted to show that the elements specified by the Examiner have been labeled. To the extent the Examiner believes that the labeling is inappropriate, or that other issues exist with the drawings, Applicant respectively requests that the Examiner either articulate the nature of the objection, or withdraw the objection.

Claim 13 has been rejected under 35 USC § 102(b) as allegedly being anticipated by Schneier. Claims 14-37, 41-44 and 46-53 have been rejected under 35 USC § 103(a) as allegedly being unpatentable over Schneier. Claims 38 and 45 have been rejected under 35 USC § 103(a) as allegedly being unpatentable over Schneier in view of Thompson (U.S. 6,282,552). Claims 24, 28-37, 39, and 40 have been further rejected under 35 USC § 112, second paragraph, as allegedly being indefinite. Claims 28 and 32 have been further rejected based on minor informalities. In view of the foregoing amendments canceling claims 1-53, these rejections are moot.

The Examiner's rejection is based primarily on Schneier. Schneier is directed to cryptographic techniques using a random session key to conduct an electronic transaction. More particularly, Schneier describes a methodology wherein one party (say a member) using an electronic card obtains another party's (say a service provider's) public key from a central database, encrypts a random session key with the service provider's public key, and sends it to the service provider. The service provider can then decrypt the communication using its private key to recover to the session key, and then the transaction can be continued

using the session key. Unfortunately, this approach, as admitted by Schneier, is vulnerable to security breaches. Accordingly, in practice, a third party Key Distribution Center (KDC) is employed to deliver the public keys, digitally signed by the KDC, to the member and service provider. This approach allows the member and service provider to each confirm that the received public key belongs to the other party by verifying the signature of the KDC.

Applicant discloses a novel and unobvious approach for cryptographic communications using an electronic card which eliminates the need for the third party KDC while maintaining a heightened level of security. Instead of storing the service provider's public key in a centralized database, as suggested by Schneier, Applicant teaches pre-loading the service provider's public key directly on the member's electronic card. With this approach, the member can directly access the service provider's public key from the electronic card without the need for the KDC. Clearly, Applicant discloses a novel and unobvious invention over Schneier.

Referring now to the specific claims, Applicant submits that they recite subject matter which is neither disclosed or suggested by Schneier. Independent claims 54, 81, 96, 103, 109 and 113 each recite, *inter alia*, a cryptographic method using "*an electronic card*" having "*a public key of a service provider*" and encrypting at least a protion of a communication from the member to the service provider using "*the service provider's public key from the electronic card*." (emphasis added). None of the cited references by the Examiner, either alone or in combination, disclose or suggest this approach. Schneier discloses the exchange of a session key using a public key. However, the public key is obtained from a central database rather than an electronic card. Based on this distinction alone, Schneier is legally insufficient to provide a basis for non-patentability of the now claimed subject matter.

In view of the foregoing amendments and remarks, it is respectfully submitted that this application is now in condition for allowance, and accordingly, reconsideration and allowance are respectfully requested.

Respectfully submitted,

Craig A. Gelfound

Craig A. Gelfound
Registration No. 41,032

McDERMOTT, WILL & EMERY
2049 Century Park East, 34th Floor
Los Angeles, CA 90067
(310) 277-4110
Facsimile: (310) 277-4730
Date: October 8, 2002

APPENDIX A

The entire SUMMARY OF INVENTION section has been amended as follows:

In one aspect of the present invention, a method of conducting an electronic transaction using an electronic card having a public key of a service provider, includes initiating a transaction at a cardholder location by encrypting at least a portion of a message with the service provider's public key from the electronic card and sending the message to a service provider location, and completing the transaction between the cardholder and the service provider in response to the message.

In another aspect of the present invention, a method of conducting an electronic transaction using an electronic card having a public key of a service provider includes formatting a key exchange request message at a member, at least a portion of the key exchange request message being encrypted using the service provider's public key from the electronic card, sending the key exchange request message from the member to the service provider, generating a session key at the service provider in response to the key exchange request message, formatting a key exchange response message including the session key at the service provider, sending the key exchange response message from the service provider to the member, and using the session key to complete the transaction.

In yet another aspect of the present invention, a method of conducting an electronic transaction using an electronic card having a public key of a service provider includes generating a member challenge by the member, encrypting by the member the member challenge using the service provider's public key from the electronic card to generate a first cryptogram, formatting by the member a key exchange request message including the first cryptogram and a public key of the member, signing digitally by the member the key exchange request message, sending the digitally signed key exchange request message to the service provider, generating by the service provider a service provider challenge, generating by the service provider a session key, encrypting by the service provider the service provider challenge and the session key using the member's public key to generate a second cryptogram, formatting by the service provider a key exchange response message including the second cryptogram and a response to member challenge, signing digitally by the service provider the key exchange response message,

sending the digitally signed key exchange response message to the member, encrypting by the member a member response for the service provider challenge using the session key to generate a third cryptogram, attaching the third cryptogram to a transaction message going from the member to the service provider, signing digitally by the member the transaction message going from the member to the service provider, and sending the transaction message going from the member to the service provider to the service provider.

In a further aspect of the present invention, a method of communication using an electronic card having a public key of a service provider includes formatting a first key exchange request message at a first member, the first key exchange request message having a public key of the first member, and at least a portion of the first key exchange request message being encrypted using the service provider's public key from the electronic card, sending the first key exchange request message from the first member to a second member, combining at a second member, a second member key exchange request message with the first member's key exchange request message and sending the combined key exchange request message, signed by the second member, to a service provider, formatting a key exchange response message at the service provider including a first session key for the first member, signing the response message, formatting a key exchange response message including a second session key for the second member, combining the key exchange response messages into a combined key exchange response message, signing the combined key exchange response message, and sending the combined key exchange response message to the second member, and separating at the second member, the key exchange response message for the second member from the key exchange response message for the first member, and forwarding the key exchange response message for the first member to the first member.

In yet a further aspect of the present invention, a method of communication using an electronic card having a public key of a service provider includes formatting a first key exchange request message at a first member, the first key exchange request message having a public key of the first member, and at least a portion of the first key exchange request message being encrypted using the service provider's public key from the electronic card, sending the first key exchange request message from the first member to

at least one intermediate member coupled in series between the first member and the service provider, each of said at least one intermediate member being either a message router or a participating member, generating, if said at least one intermediate member comprises at least one participating member, at each of the participating members a key exchange request, receiving at the service provider a combined key exchange request message from said at least one intermediate member, the combined key exchange request message comprising the first key exchange request message and the key exchange request message generated by each of the participating members, generating at the service provider a first session key for the first member and a participating session key for each of the participating members, formatting at the service provider a key exchange response message including each of the first and participating session keys, sending the key exchange response message from the service provider to said at least one intermediate member, separating by each participating member its respective participating session key from the key exchange response message, and sending the first session key from said at least one intermediate member to the first member.

In another aspect of the present invention, a method of communication using an electronic card having a public key of a service provider includes formatting a key exchange request message at each of a plurality of first members, the key exchange request message for one of the first members having a public key of said one of the first members, and at least a portion of the key exchange request message for said one of the first members being encrypted using the service provider's public key from the electronic card, sending from each of the first members its respective key exchange request message to a second member, the second member being either a message router or a participating member, generating, if the second member is a participating member, a second key exchange request message at the second member, combining at the second member the key exchange request message from each of the first members to form a combined key exchange request message, the combined key exchange request message further comprising the second key exchange request message if the second member is a participating member, receiving at the service provider the combined key exchange request message from the second member, generating at the service provider a first session key for each of the first members, and a second session key for the second

member if the second member is a participating member, formatting at the service provider a key exchange response message including each of the first and second session keys, sending the key exchange response message from the service provider to the second member, separating by the second member the second session key from the key exchange response message if the second member is a participating member, separating by the second member the first session key for each of the first members from the key exchange response message, and sending each of the first session keys to its respective first member.

[In one aspect of the present invention, the system for electronic transactions comprises: an electronic card having a cryptographic service for encryption and decryption, a data area for storing cardholder information, and a data area for storing service provider information; a service provider member terminal responsive to activation of the electronic card; and a service provider terminal in communication with the service provider member terminal, the service provider terminal decrypting communication from the service provider member terminal and encrypting communication to the service provider member terminal, the service provider member terminal encrypting communication to the service provider terminal and decrypting communication from the service provider terminal.

In another aspect of the invention, the method of conducting an electronic transaction using an electronic card comprises formatting a key exchange request message at a member, sending the key exchange request message from the member to a service provider, generating a session key at the service provider, formatting a key exchange response message including the session key at the service provider, sending the key exchange response message from the service provider to the member and using the session key to conduct a transaction.

In yet another aspect of the invention, the method of conducting an electronic transaction using an electronic card comprises formatting a key exchange request message at a member, the key exchange request message has a member challenge for the service provider, sending the key exchange request message from the member to a service provider, generating a session key at the service provider, formatting a key exchange response message including the session key at the service provider, the key

exchange response message has a response for the member challenge and a service provider challenge for the member and sending it to the member, formatting by the member a response for the service provider challenge and sending it to the service provider and using the session key to conduct a transaction.]

O I P E JC61 OCT 15 2002 PATENT & TRADEMARK OFFICE

Docket No. 064808-011

I certify that on **October 8, 2002**, which is the date I am signing this certificate, this correspondence and all attachments mentioned are being deposited in the United States Postal Service first-class mail in an envelope addressed to: Commissioner of Patents, Washington, D.C. 20231.

Marie W. Lau

PATENT
Applicant: Chen, Jay C.
Serial No.: 09/456,794
Filing Date: December 8, 1999
Title: A CRYPTOGRAPHIC SYSTEM AND METHOD FOR ELECTRONIC TRANSACTIONS
Group Art Unit: 2132
Examiner: Meislahn, Douglas

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner of Patents
Washington, D.C. 20231

TRANSMITTAL OF AMENDMENT

Sir:

We enclose the following documents relating to the above-identified patent application:

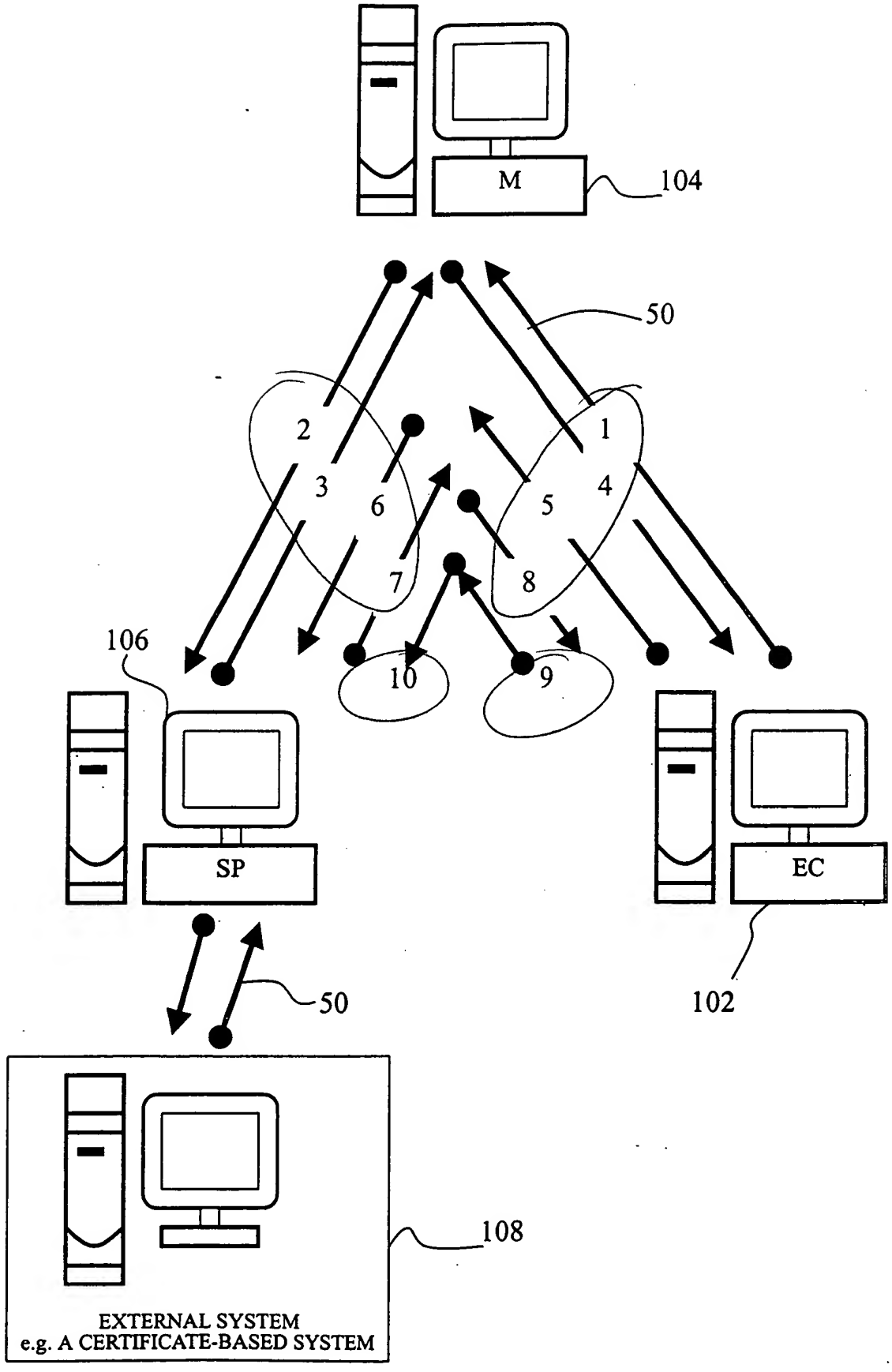
1. Response to Office Action dated July 2, 2002;
2. Petition of Extension of Time
3. Applicant authorizes the additional fees to be charged to deposit account number 501946 (Order No. 64808-011) in the name of McDermott Will & Emery. A duplicate of the document is enclosed.

Craig A. Gelfound, Reg. No. 41,032
Attorney for Applicant
310-277-1533

MCDERMOTT, WILL & EMERY
2049 Century Park East, 34th Floor
Los Angeles, CA 90067
Telephone: (310) 277-4110 • [fax] (310) 277-4730

OIPE JC81 OCT 15 2002 PATENT & TRADEMARK OFFICE

FIG. 2



OIPE JC81
OCT 15 2002
PATENT & TRADEMARK OFFICE

FIG. 12